EU criminal law and the regulation of information and communication technology

Summers, Sarah

Abstract: The opportunities afforded by the global information space give rise to the potential for the commission of new crimes –crimes such as hacking or denial of service attacks– and for existing crimes, such as speech offences or fraud, to be committed in new ways and with potentially larger consequences. One of the biggest challenges for the regulation of information and communications technology is that the global information space does not respect national boundaries. In order to be successful, any regulatory approach will call for some degree of cooperation between countries. This poses an obvious problem for those seeking to develop a regulatory structure. This challenge is particularly relevant in the criminal law context, as the criminal law has traditionally been considered to be the product and responsibility of national law. This article considers the EU's regulatory approach in this area. The aim here is not to offer a critique of the EU's regulatory structure in the context of cybercrime, but rather to use the situation in the EU to illustrate various issues arising in the context of the criminal law regulation of information and communications technology. This article examines some of the issues which have arisen in the context of the regulation of cyber activity at the EU level as a result of this tension between national sovereignty and broader overarching EU regulation and assesses the relevance of these issues in the context of criminal law regulation more broadly. Consideration of the processes of criminalisation and harmonisation provides the basis for an analysis of the manner in which the EU seeks to justify its involvement in criminal law in this field.

DOI: https://doi.org/10.15845/bjclcj.v3i1.827

Bergen Journal of Criminal Law and Criminal Justice • Volume 3, Issue 1, 2015, pp. 48-60

EU Criminal Law and the Regulation of Information and Communication Technology

*SARAH SUMMERS**

1 Introduction: Criminal law regulation in the context of information and communication technology

It is well known that the opportunities afforded by the global information space give rise to the potential for the commission of new crimes –crimes such as hacking or denial of service attacks– and for existing crimes, such as speech offences or fraud, to be committed in new ways and with potentially larger consequences. The most interesting aspect of cybercrime regulation for criminal lawyers is the suggestion that individual countries cannot effectively unilaterally create and enforce criminal laws to regulate such matters. Perhaps the biggest challenge for the regulation of information and communication technology (ICT) is that the global information space does not respect national boundaries. There is clear potential for national legislation in the UK or Switzerland or Norway to be undermined by a less strict regulatory regime elsewhere. It seems likely that in order to be successful, any regulatory approach will call for some degree of cooperation between countries. This poses an obvious problem for those seeking to develop a regulatory structure. This challenge is particularly relevant in the criminal law context, as the criminal law has traditionally been considered to be the product and responsibility of national law.

Even if we accept the need for some kind of overarching criminal law regulation, questions arise as regards the group or organisation which is best placed to develop these provisions and the means by which these are to derive their legitimacy. It is this tension between national sovereignty on one hand and the need for common cross border regulation on the other, which is so clearly evident in the context of cyber-criminality.

* SNSF Professor, University of Zurich, Switzerland. This article is based on a paper presented by the author at the Bergen Lecture on Criminal Law and Criminal Justice in 2014.

These issues are well illustrated in the attempts of the EU to develop criminal law regulation in this field. The EU has focused considerable attention in the context of the criminal law on the regulation of cybercrime. This is not particularly surprising as the cross-border nature of cybercrime provides the EU with justification for action. But there seems to be something of an inherent contradiction in this regard: the global reach of cybercrime may well be said to give the EU a mandate for action, but in doing so it immediately raises the question as to whether a regional body has the capacity to regulate an issue which is essentially global in nature.

The focus of this article will be the EU's regulatory approach. The aim here is not to offer a critique of the EU's regulatory structure in the context of cybercrime, but rather to use the situation in the EU to illustrate various issues arising in the context of the criminal law regulation of information and communication technology. It is important to note that while the EU often refers to the information society, this concept is left undefined. This lack of definition might be explained by the fact that there is no single, universally accepted theory of the nature and characteristics of the information society.[1] Indeed it could be argued that the somewhat blurry nature of the term information society led to its popularity in EU policymaking circles and to the usage of the term for political purposes "to enhance the standing of the Commission as an actor in a governance matrix as opposed to a hierarchical system of governments within the EU." [2] This paper will not set out a comprehensive descriptive account of EU ICT developments, nor will it provide an overview of EU criminal law regulation. Instead, some of the issues which have arisen in the context of the regulation of cyber activity at the EU level as a result of this tension between national sovereignty and broader overarching EU regulation will be examined, and the relevance of this in the context of criminal law regulation more broadly will be assessed. Consideration of the processes of criminalisation and harmonisation will enable an analysis of the manner in which the EU seeks to justify its involvement in criminal law in this field.

2. Criminalisation

In the context of the criminalisation of cyber-activity, any supra-national approach to criminalisation presupposes that a consensus can be reached on what should be criminalised and the extent of such criminalisation.

1 See further Webster, *Theories of Information Society* (Routledge 1995) identifying five definitions of the information society – technological, economic, occupational, spatial, cultural – all of which are found wanting; May, *The Information Society: A Sceptical View* (Polity Press, 2002).

2 Shahin & Finger, The History of a European Information Society: Shifts from Government to Governance, in *Advancing e-governance through innovation and leadership,* eds. Tubtimhin & Pipe, (IOS Press 2009) 62.

The fact that the EU has frequently relied on the cross-border dimension of crime to justify its involvement in the criminal law means that much of the legislation which it has adopted has relevance in the context of the regulation of ICT. If we look at the various areas of criminal law subject to the attention of EU regulators, we can see that some provisions are obviously directly related to cybercrime: for instance the provisions of the Directive on Attacks against Information Systems, or those in the Fraud and Counterfeiting Framework Decision.[3] Even in relation to legislative instruments which are not –or not principally– concerned with the regulation of the information environment, such as the Framework Decision on Terrorism, or the Directive on Combatting the Exploitation of Children, the Internet in particular plays an important role. The Directive on the Exploitation of Children has distinct provisions concerning online grooming,[4] and the terrorism legislation was designed partly in response to fears of online incitement to violence.[5]

Within the EU there are varying degrees of acceptance about the types of cyber-activity which ought to be criminalised. In the context of some types of activity –such as conduct which is connected to the production or display of child pornography– there is broad acceptance of some role for criminal law. Similarly there is a wide consensus concerning the necessity of criminalising various activities which can broadly be characterised as amounting to or contributing to cyber-attacks against information systems. In relation to such crimes, as we shall see, the discussion has focused on the extent of criminalisation rather than the need for criminal law in the first place. In relation to some other areas, however, there is widespread disagreement about the resort to criminal law in the first place – this is most evident in the context of the EU's attempts to create criminal law designed to tackle intellectual property violations. It is worth dwelling briefly on the EU's IP criminal law saga as this highlights many of the problems associated with criminalisation at the EU level.

3 Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, O.J. 2013, L 218/8, Arts 3-8; Framework Decision 2001/414/JHA of 28 May 2001 on combating fraud and counterfeiting of non-case means of payment, O.J. 2001, L 149/1, Art. 3.

4 Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA, O.J. 2011, L 335/1, Arts 4-7.

5 Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, O.J. 2002, L 164/4, as amended by Framework Decision 2008/919/JHA of 28 November 2008, O.J. 2008, L 330/21, Recital 4: 'The Internet is used to inspire and mobilise local terrorist networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a "virtual training camp". Activities of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism have multiplied at very low cost and risk.'

The EU has produced a whole host of provisions with relevance for the regulation of intellectual property. Copyright in particular has been subject to considerable attention – this is perhaps unsurprising in view of the potential for piracy in light of increasing digitalisation. This was made clear in the green paper on copyright in the information society which was published in 1995.[6] The principal focus of the regulatory approach was not piracy but rather the prevention of the fragmentation of the internal market. In order to avoid this, the Commission sought to harmonise the sanctions to be imposed for copyright infringement and in this context planned to 'approximate' criminal law sanctions.[7] It is important to stress that criminal law concerns were definitely not at the forefront of the regulators' concerns – rather they were seen as additional measures which could also prove useful in promoting the interests of the internal market. The EU has since enacted a series of directives and regulations on intellectual property, not to mention a vast quantity of supplementary legislation.

In its proposal for a Directive on Measures to ensure the Enforcement of Intellectual Property (IPRED; Enforcement Directive) published in 1998 the Commission noted that while all of the Member States had, in line with the TRIPS Agreement, introduced criminal laws to protect intellectual property, there were considerable differences between the Member States as regard the imposition of criminal penalties.[8] According to the Commission, "the effective application of genuinely deterrent sanctions in all Member States would help greatly in combating counterfeiting and piracy."[9] The criminal law provisions of the proposal were set out in Article 20:[10]

> *1. Member States shall ensure that all serious infringements of an intellectual property right, as well as attempts at, participation in and instigation of such infringements, are treated as a criminal offence. An infringement is considered serious if it is intentional and committed for commercial purposes.*
> *2. Where natural persons are concerned, Member States shall provide for criminal sanctions, including imprisonment.*

In view of the fact that the Commission's aim was to harmonise criminal penalties, the fact that these were not mentioned in the provision is notable. This was due of course to

6 COM (95) 382 final, Green paper on Copyright and related rights in the Information Society.

7 Ibid, p. 51.

8 COM (2003) 46 final, Proposal for a Directive on measures and procedures to ensure the enforcement of intellectual property rights, Brussels, 30 January 2003, pp. 15-16.

9 *Ibid.*, p. 16.

10 The Legal Committee of the European Parliament supported this version, see: European Parliament's Committee on Legal Affairs and the Internal Market, Report on the proposal for a directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights (COM(2003) 46 – C5-0055/2003 – 2003/0024(COD)), 5 December 2003, A5-0468/2003, no 43.

the fact that at that point in time the EU did not have competence in the context of the first pillar to create criminal law.[11] Nevertheless it does seem to call into question to some extent the point of the provision.

Agreement on the article proved, in any event, to be extremely difficult to secure and the criminal law provisions in the Enforcement Directive were dropped from the version of the Directive that was subsequently enacted. There were similar problems with the subsequent attempts to enact criminal law provisions in an amended proposal for a second Enforcement Directive (IPRED2) in 2006.[12] By this time the Commission was focused very much on piracy and sought to strengthen its case for action by arguing that it was connected to organised crime.

Article 3 of the proposed directive would have required the Member States to ensure that all intentional infringements of intellectual property rights on a commercial scale were treated as criminal offences. In addition a provision was to be made for the criminalisation of attempts, aiding and abetting and the incitement of such infringements. The Member States would have been required, in line with Article 4, to provide for the imposition of fines for both natural and legal persons. In addition, they would have obliged to provide for maximum custodial sentences for natural persons of at least four years. This reference to the penalties to be imposed emphasises the growing confidence of the Commission in its regulation of the criminal law; well-placed as it turns out –as made clear by the ECJ's judgments in the environmental crime cases.

Although initially welcomed by the European Parliament,[13] the proposal was never adopted. This was mainly due to the controversy surrounding the criminal law competence of the EU which meant that there was no consensus in the Council in favour of the proposal.[14] In 2010, the Commission withdrew the proposal[15] on the basis that it was

11 On the competence saga, see Summers *et al.*, *The Emergence of EU Criminal Law* (Hart Publishing 2014), p. 38ff.; Wasmeier & Thwaites, The Battle of the Pillars: Does the European Community have the Power to Approximate National Criminal Laws?, 29 EL Rev (2004) p. 613.

12 Proposal for a Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights, Brussels, 12.7.2005, COM (2005) 276 final; Amended proposal for a Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights, Brussels, 26.4.2006, COM (2006) 168 final.

13 European Parliament legislative resolution of 25 April 2007 on the amended proposal for a Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights (COM(2006)0168 – C6-0233/2005 – 2005/0127(COD)), P6_TA(2007)0145.

14 See e.g. Ackermann, Immaterialgüterstrafrecht, in *Wirtschaftstrafrecht der Schweiz*, eds. Ackermann & Heine (Stämpfli 2013), p. 731.

15 Withdrawal of obsolete Commission Proposal 2010/C 252/04; List of proposals withdrawn [2010] OJ C 252/7.

unlikely to be able to secure the implementation of the directive in the near future. [16] It did so not because of uncertainty about whether it thought the criminal law measures were necessary, but because it planned to achieve the same result by promoting the ratification of the Anti-Counterfeiting Trade Agreement (ACTA),[17] which set out various provisions on criminal penalties for intellectual property right violations in Articles 23 and 24. In mid-2011, the Commission recommended that the EU ratify ACTA,[18] but the European Parliament refused to do so as it was concerned by the continuing protests and reservations about the Agreement. One of these addressed to the European Parliament demanded that its Members 'stand for a free and open Internet' and was signed by over 2.8 million people. A vote on the ratification of ACTA was resoundingly rejected: 478 Members of Parliament voted against the Agreement, while only 39 MEPs were in favour and 165 MEPs abstained. [19]

This whole episode is of particular relevance as it demonstrates clearly that the Commission did not pay much attention to the importance of setting out the case for criminalisation. Rather it determined that variation in criminal law regulation could cause fragmentation of the internal market and then scrambled to find a few reasons to justify the EU's involvement in setting out criminal law provisions, such as the cross border nature of crime, deterrence and so on. It did not however engage with difficult questions about the case for criminalisation; about whether criminal law should be used to sanction IP right violations, about the extent of any resort to the criminal law and crucially about whether the criminal penalties were likely to improve compliance with EU law.[20] In the absence of consensus on the need for criminal law in the first place, however, it seems likely that it will be impossible to achieve agreement on over-arching provisions at the European level.

Even in relation to those areas in which there might be said to be recognition of the need for criminal law regulation, such as the regulation of racist content or incitement to racial hatred in the online environment for instance, there is widespread disagreement between

16 Walter & Goebel, Enforcement Directive, in *European Copyright Law: A Commentary,* eds. Walter & von Leweinski (Oxford University Press 2010), p. 13.

17 See also Geiger, Weakening Multilateralism in Intellectual Property Lawmaking: a European Perspective on ACTA, in 3 *The WIPO Journal* (2012), p. 166, at 167.

18 Proposal for a Council Decision on the conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, Brussels, 24.6.2011, COM (2011) 380 final.

19 Plenary Session Press release, European Parliament rejects ACTA, 04.07.2012, available at http://www.europarl.europa.eu/news/en/news-room/content/20120703IPR48247/html/European-Parliament-rejects-ACTA. [Last accessed 30 June 2015]

20 On this notion of effectiveness, see Öberg, Do we really need Criminal Sanctions for the Enforcement of EU Criminal Law, in *New Journal of European Criminal Law* (2014), p. 370, at 378.

countries about the extent of any such regulation. It took almost a decade, for instance, for agreement to be reached on the Framework Decision on combating certain forms of Racism and Xenophobia – largely because of differences between the Member States on criminalisation of speech offences and the role and understanding of the freedom of expression guarantee. The UK, which has a long history of resisting pure speech offences was worried about the 'excessively subjective' nature of the proposed provisions and the fact that it did not call for offences to be incited in order for criminal liability to arise. The Framework Decision was finally enacted after compromise was reached in 2008. This consensus, however, did not last long: Following the entry into force of the Lisbon Treaty, the UK opted out of all of the Instruments of the third pillar and the UK Government intimated that it did not intend to re-join measures establishing minimum requirements for the constituent elements of racism and xenophobia.[21]

There was also a lack of agreement on subsidiary-regulatory measures which might give rise to criminal liability in the event of non-compliance such as requirements that ISPs take certain action if they are aware of unlawful content, or requirements that they block certain websites. Filtering and blocking content might seem proportionate in certain cases but there is clearly potential for a chilling effect on free speech – particularly if ISPs and other operators in the information society feel obliged to take sweeping and indiscriminate action to avoid liability.

This disagreement —or at least lack of consensus— about criminalisation and its scope, focuses attention on the process by which the need for, and extent of, criminal law is determined. In national legal systems such processes involve the formation of working groups and expert committees. In the EU on the other hand it is often difficult to trace the development of the Commission's proposals. Indeed the Commission has had a tendency to rely on management consultancies and academic reports funded by EU institutions and there appears to be considerable scope for lobbying groups based in Brussels to intervene.

The case for criminalisation has been neglected. Questions about the necessity or proportionality of criminal law go to the very essence of the criminal law debate and to the understanding of any resort to criminal law as being guided by the ultima ratio principle. This seems at times to be entirely missing in the EU debate and sometimes also at the national level, it must be conceded, as legislatures scramble to enact new legislation in response to the perceived need to respond to new challenges. This is particularly evident in relation to the intellectual property directives, because the EU's regulatory approach was not focused on the criminal law per se, but rather on preventing diversity in the criminal laws of the Member States having a negative impact on the internal market.

[21] House of Commons European Scrutiny Committee, *The UK's Block Opt-out of pre-Lisbon Criminal Law and Policing Measures*, 21st Report of Session 2013-14, HC 683 (2013), p. 10.

This is likely to become increasingly relevant in the future in view of the express basis in Article 83(2) TFEU for the creation criminal laws to ensure the effective implementation of EU policy.[22]

3. Harmonisation

Difficulties arise not just in relation to criminalisation but also in the context of harmonisation. The need for EU criminal law legislation in the field of ICT is based on the assumption that the EU is better placed to regulate such matters than the Member States acting on their own. This presupposes, as mentioned above, that agreement can be reached on the determination of what should be criminal and the extent and limits of such criminalisation. But even if such consensus is achieved, questions arise as to how much harmonisation is necessary and whether in fact harmonisation is even possible. If harmonisation is not possible, what does this mean for the EU's legislative forays into the regulation of ICT or for the supra-national regulation of ICT more broadly?

In those areas in which there is no consensus on criminalisation, harmonisation is of course impossible; but even in those areas where there is broad consensus, questions remain as to the possibility of harmonisation. This can be well illustrated by way of some examples. If we look at the EU legislation on attacks against information systems for instance, an area in which criminalization enjoys considerable support, we can see that implementation of the original legislation – the now repealed Framework Decision – was patchy. The initial Framework Decision outlined three principal offences designed to develop national laws to counter 'hacking'. Illegal access to information systems: 'intentional access without right to the whole or any part of an information system';[23] Illegal system interference: 'intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data… when committed without right;'[24] and Illegal data interference: 'intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system.'[25] It is notable though that the Member States were only obliged to provide for the imposition of criminal sanctions in relation to those cases which were deemed to be 'not minor'.[26]

These offences are essentially reproduced in the subsequent Directive which repealed and replaced the Framework Decision and which was adopted to address 'new' threats,

22 See further *Summers et al.* 2014, ch 2.

23 Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems, Art 2(1), O.J. 2005, L 69/67.

24 *Ibid.*, Art 3.

25 *Ibid.*, Art 4.

26 *Ibid.*, Recital 17.

in particular the threat of 'massive simultaneous attacks against information systems' and the emergence of 'botnets.' [27] In addition the Directive requires Member States to criminalise the intentional interception 'by technical means' of 'non-public transmissions of computer data to, from or within an information system,' [28] and the 'intentional production, sale, procurement for use, import, distribution or otherwise making available, of' certain tools for committing the offences.[29]

In the context of the Framework Decision, the Member States were obliged to impose 'effective, proportional and dissuasive' penalties,[30] and in relation to system interference and data interference offences, maximum sentences of between one and three years in prison. The Directive introduces a broader range of penalties. In addition to 'effective, proportionate and dissuasive penalties,' the Member States must also provide for maximum sentence of imprisonment of at least two years in such cases 'which are not minor.' [31] In the context of system and data interference, the Member States must ensure that the offences are punishable by 'a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, designed or adapted primarily for that purpose' [32] and by a maximum sentence of at least 5 years if committed within the framework of a criminal organisation, if they cause serious damage or if they are committed against a critical infrastructure information system.' [33]

As many commentators have noted minimum levels for maximum sentences are of limited relevance in the harmonisation process because of the wide margin of appreciation left to the Member States.[34] Indeed we can see here in the short period between the enactment of the Framework Decision and the subsequent enactment of the Directive a doubling of the minimum maximum sentence, without any detailed explanation as to why this is necessary, beyond throwaway comments about the need for deterrence. There is not yet any data on the implementation of the Directive but in its implementation re-

27 Proposal for a Directive of the European Parliament and of the Council on Attacks Against Information Systems and repealing Council Framework Decision 2005/222/JHA, Brussels, 30.9.2010, COM(2010) 517 final.

28 Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, O.J. 2013, L 218/8 Art. 6.

29 *Ibid.*, Art 7.

30 O.J. 2005, L 69/67, Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems, Art 6(1).

31 *Ibid.*, Art 9(1) and (2).

32 *Ibid.*, Art 9(3).

33 *Ibid.*, Art 9(4).

34 For discussion of divergence in the implementation of minimum maximum sentences in the context of money laundering, see Alexander, *Insider Dealing and Money Laundering in the EU: Law and Regulation* (Ashgate 2007), p. 148.

port on the Framework Decision the Commission noted that it had been 'implemented in very different ways in the 20 Member States,' that 'the legal concepts and expressions used' in implementing the legislation were 'not easily comparable'[35] but noted in general that progress had been made.

In view of the fact that the Member States were only required to criminalise 'non minor' conduct, there was obviously room for substantial disparity to creep in. The Commission addressed this in its implementation report. In the context of the illegal accessing of information systems, for instance, it noted that various Member States had restricted liability to those cases which they perceived to be non-minor in nature. In Austria, the legal criterion for criminal responsibility was such that intent to perpetrate data espionage and to use the data obtained in order to make a profit or to cause damage had to be at hand. The Czech Republic had criminalised illegal access only in cases in which the data were subsequently misused or damaged. Finland, meanwhile, had interpreted the position to include the requirement that the data accessed had actually been 'endangered,' while in Latvia, illegal access was only to be criminalised if substantial injury had thereby been caused.[36]

The Commission noted that a definition of 'cases which are not minor' was necessary in order to determine compliance with the provision, went on to define minor cases as 'cases where instances of illegal access are of minor importance or where an infringement of information system confidentiality is of a minor degree' and concluded that all four member states had not correctly implemented the provisions.[37] This is all somewhat confusing; clearly the notion of 'non-minor' cases should have been included in the EU legislation if the provisions were to be implemented at all uniformly. Further, and perhaps more importantly, even assuming that the Member States were to enact the legislation to the letter, there is considerable room for diversity. Even in the event of wide-scale implementation, the question is whether true harmonisation of the criminal law can be achieved without the harmonisation of the general principles of criminal law.

The Directive refers only to intentional conduct but there is no definition of intent. This is of considerable relevance in the context of any attempt to 'harmonise' the criminal law of the Member States. If in the context of the definition of the 'subjective' component of a criminal offence, we compare, for instance, the position in Scotland and in Switzerland we can see that there are considerable differences.

35 Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, Brussels, 14 July 2008, COM (2008) 448, 2.1.

36 *Ibid.*

37 *Ibid.*

The attribution of criminal liability in Scotland, for instance, requires the concurrence of mens rea and actus reus.[38] There are various degrees of mens rea – the state of mind of the offender at the time of the commission of the offence – including intent, recklessness and negligence. Swiss criminal law, on the other hand, relies on a tripartite conception of criminal liability (*Tatbestandsmässigkeit, Rechtswidrigkeit, Schuld*). In Swiss law, the attribution of liability requires that the offender act either with intention (*Vorsatz*) or negligence (*Fahrlässigkeit*).[39] But even the most cursory of glances at these concepts demonstrates that intention in Scotland is not the same as intention in Switzerland. The notion of dolus eventualis (the offender was aware of the risks and took these risks into account when acting), for example, is considered to be a form of intent in Swiss law, but would not be classed as a form of interest in Scotland as it would rather fall within the concept of recklessness. This means that, assuming the Member States followed the EU's instructions, any requirement to criminalise intentional conduct would result in broader criminalisation in Switzerland than in Scotland.

This has consequences which go beyond merely intention – but extend (as a result of the dominant theories) across many of the general principles of the criminal law. The Member States are required to provide for criminal liability for the attempt to commit a crime set out in Articles 4 and 5.[40] But there is no definition of the term 'attempt' in the Directive, despite wide variations in the regulation of attempts across the Member States. Similar issues apply in the context of incitement or aiding and abetting and with regard to the definition of notions such as participation in crime or the criminal liability of legal persons.

Whether the lack of a common understanding of the general principles of the criminal law is deemed to be problematic depends, of course, on the nature of the harmonisation which the supra-national regulating authority seeks to achieve. If approximation of laws is neither desired nor required, then it could be argued that a simple a list of offences would be sufficient and result in a similar level of harmonisation as is currently being achieved by way of the EU Framework Decisions and Directives.

38 See Gordon, *The Criminal Law of Scotland*, ed. Christie (3rd ed., Green 2000), vol.1, p.275

39 See Stratenwerth, *Allgemeiner Teil I: Die Straftat,* (4th ed., Stämpfli 2011), § 9, N. 101, p. 203.

40 Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, O.J. 2013, L 218/8, Art. 6, Art. 8(2).

4. Conclusions: Criminal Law and the Regulation of ICT

The EU's forays into the regulation of the criminal law are very often justified by reference to the borderless nature of some types of crime as made possible by technological advances in ICT. This creates problems for national law enforcement and is said to justify the need for EU action. It is notable however that crime does not stop at the borders of the EU. Indeed, according to the former Director of Europol's Cybercrime Centre, the 'majority of cybercrime kingpins' are located in the Russian-speaking world.[41] This suggests that it is questionable whether the borderless nature of cybercrime really justifies EU involvement. It also gives rise to the suspicion, as some commentators have suggested, that the EU is using developments in the information society as an excuse to justify its involvement in the criminal law and thereby establish itself as a legitimate political force.

There can be little doubt that the borderless nature of cyber-activity gives rise to problems for those charged with creating and enforcing criminal law. This overview of the EU's regulatory approach highlights various issues which must be considered in addressing this challenge:

First, any supra-national regulation of the criminal law must focus on the reasons for criminalisation, as is well illustrated by the failed attempts to establish criminal law provisions to address intellectual property violations. On the one hand this involves taking seriously the importance of making the case for criminalisation, on the other it focuses attention on the socio-political aspects underlying the criminal law. The EU's overt focus on promoting the free market and the principles of liberalisation, which had been accepted without any resistance in the context of civil law provisions, resulted in considerable opposition as soon as it was transposed into the criminal law provisions.

Second, in the context of the regulation of ICT, the criminal law has not been at the forefront of the EU's concerns, but has rather been something of an afterthought. Indeed, the EU's regulation of cyber-activity highlights the fact that the criminal law is, if not exactly subsidiary, certainly only one weapon in the EU's regulatory arsenal. In modern times when criminal law is often wheeled out as a supposed remedy for all of society's ills, it is rather refreshing to be confronted with the subsidiary nature of EU criminal law. Alas, the fact that the criminal law is not the primary concern of EU regulators does not automatically imply endorsement of the ultima ratio principle, nor acknowledgment of necessity or proportionality concerns in the context of the creation of EU criminal law. These however must be at the forefront of criminal law regulation.

41 See the article on the BBC News Website: http://www.bbc.com/news/technology-29567782 [last accessed 20.3.15]

Third, the EU's endeavours in matters concerning the criminal law emphasise the difficulty of achieving consensus in criminal legal matters outside of the traditional sphere of political democracy in the nation state. Criminal law is essentially a political matter and any attempt to regulate it must deal with the relationship between the state and its citizens. This will inevitably prove problematic for any attempt at supra- or indeed inter-national regulation. In the words of the German Constitutional Court: "Democratic self-determination is affected in an especially sensitive manner by provisions of criminal law and criminal procedure, the corresponding basic powers in the treaties must be interpreted strictly… and their use requires particular justification."[42] This care as regards criminalisation is absent at the EU level and it is questionable whether it is even achievable in the current political set-up of the EU.

This all focuses attention back to the aims and extent of criminalisation and harmonisation. It is questionable whether the type of harmonisation sought by the EU is required, desired or is even achievable in the manner currently employed. In fact it might well be argued that a simple list of criminal offences would result in a similar degree of harmonisation as is currently being achieved by the EU, would be sufficient to facilitate the prosecution of cross-border crime and would be considerably less controversial. Further, in view of the difficulties of achieving consensus in the EU, the likelihood of securing broader global consensus seems extremely small. A less aggressive approach to criminal law regulation –one less tied up with the EU's attempts to establish itself politically– might enable broader consensus and wider global reach.

42 BVE 2/08, 30 June 2009, para. 358.